What is claimed is:

Sub a1

1. A method for generating an authentication tag for a message, comprising:

(a) processing a portion of the message using a first function to produce an interim output; and

(b) processing the interim output using a second function to produce the authentication tag.

2. A method according to claim 1, wherein the message includes a number of message parts, and wherein the portion of the message processed is selected by using a pseudorandom probabilistic function to determine whether each message part is provided as input to said first function.

3. The method of claim 2, wherein said message parts are 64-bit words.

4. A method according to claim 1, further comprising partitioning the message into regions, each region including a number of message parts, and providing one message part from each region as input to said first function.

5. A method according to claim 1, wherein the message includes a number of message parts, and wherein the portion of the message processed is selected by:

defining a message selection percentage p; and

using a pseudorandom probabilistic function, uniform over an interval [1, 2L], where L = 1/p and p is a message selection percentage, to determine offsets between message parts which are provided as input to said first function.

6. A method according to claim 1, wherein said first function is a keyed hash function.

7. A method according to claim 1, wherein the cryptographic hash function is one of an MD4 hashing function, a bucket hashing function, a multilinear modular hashing function, a cyclic redundancy code-based hashing function, and an alternative hash algorithm.

8. A method according to claim 1, wherein the portion of the message processed is selected by truncating the message.

9. A device for generating an authentication tag for a message, comprising:

a first hashing module that processes a portion of the message to produce an interim output; and

a second hashing module that processes said interim output to produce the authentication tag.

10. A device according to claim 9, wherein the message includes a number of message parts, and wherein the portion of the message processed is selected by using a pseudorandom probabilistic function to determine whether each message part is provided as input to said first hashing module.

11. The device of claim 10, wherein said message parts are 64-bit words.

12. A device according to claim 9, further comprising partitioning the message into regions, each region including a number of message parts, and providing one message part from each region as input to said first hashing module.

13. A device according to claim 9, wherein the message includes a number of message parts, and wherein the portion of the message processed is selected by:

defining a message selection percentage p; and

using a pseudorandom probabilistic function, uniform over an interval [1, 2L], where L = 1/p and p is a message selection percentage, to determine offsets between message parts which are provided as input to said first hashing module.

14. A device according to claim 1, wherein said first hashing module includes a keyed hash function.

15. A device according to claim 1, wherein said first hashing module includes one of an MD4 hashing function, a bucket hashing function, a multilinear modular hashing function, a cyclic redundancy code-based hashing function, and an alternative hash algorithm.

16. A device according to claim 1, wherein the portion of the message processed is selected by truncating the message.